John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Wills Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
Email: abm@murphylegalfirm.com

**Pro Hac Vice* application to be submitted

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

CYNTHIA REPLOGLE, individually and on behalf of all others similarly situated, Plaintiff, v. EP GLOBAL PRODUCTION SOLUTIONS, LLC d/b/a ENTERTAINMENT PARTNERS, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Cynthia Replogle ("Plaintiff"), individually and on behalf of all others similarly situated, and on behalf of the general public, brings this Class Action Complaint, against defendant EP Global Production Solutions, LLC d/b/a Entertainment Partners (referred to herein as "Entertainment Partners" or "Defendant") based on personal knowledge and the investigation of counsel, and alleges as follows:

I. INTRODUCTION

1. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused Plaintiff and similarly situated persons in the preventable data breach of Defendant's inadequately protected computer network.

2. On or about June 30, 2023, Entertainment Partners identified unusual activity on its computer network, indicating a possible data breach. Following an investigation, Entertainment Partners determined that cybercriminals had infiltrated its inadequately protected network and acquired database files containing the sensitive and personal information of Plaintiff and Class members ("Data Breach" or "Breach").[1]

3. According to Entertainment Partners, the personal information acquired by cybercriminals in the Data Breach includes names, addresses, Social Security numbers, and/or tax identification numbers ("PII" or "Personal Information") of at least 471,362 individuals.[2]

4. Entertainment Partners provides "production tools and services" to "tens of thousands of productions" within the entertainment industry.[3]

[1] https://oag.ca.gov/system/files/Sample%20Individual%20Notice.pdf.

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/6dd29d7e-9e44-4ad0-9d48-1e0bd6122ab6.shtml.

[3] https://www.ep.com/company/about-us/.

5. Plaintiff and Class Members are current and former employees of Entertainment Partners and/or production companies that contracted with Entertainment Partners for services.

6. To receive employment opportunities, Plaintiff and Class members provided their PII to Defendant with the reasonable expectation that Defendant would keep that sensitive data secure.

7. By taking possession and control of Plaintiff's and Class members' Personal Information, Defendant assumed a duty to securely store and protect the Personal Information of Plaintiff and the Class.

8. Defendant breached this duty and betrayed the trust of Plaintiff and Class members by failing to properly safeguard and protect their Personal Information, thus enabling cyber criminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

9. Defendant's misconduct – failing to implement adequate and reasonable measures to protect Plaintiff's and Class members' Personal Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that it did not have adequate security practices in place to safeguard the Personal Information, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiff and Class members across the United States.

10. Due to Defendant's negligence and failures, cyber criminals obtained and now possess everything they need to commit personal identity theft and wreak havoc on the financial and personal lives of more than 470,000 individuals, for decades to come.

11. Plaintiff brings this class action lawsuit to hold Defendant responsible for its grossly negligent—indeed, reckless—failure to use statutorily required or

reasonable industry cybersecurity measures to protect Class members' Personal Information.

12. As a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class members are now forced to deal with the danger of identity thieves possessing and using their Personal Information.

13. Additionally, Plaintiff and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

14. Plaintiff brings this action individually and on behalf of the Class and seeks actual damages and restitution. Plaintiff also seeks declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper.

15. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims for (i) negligence, (ii) breach of implied contract, (iii) violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*., and (iv) violation of the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq*.

II. THE PARTIES

16. Plaintiff Cynthia Replogle is a citizen and resident of San Luis Obispo County, California.

17. Defendant is a Delaware limited liability company with its principal place of business located at 2950 North Hollywood Way, Burbank, California 91505.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has jurisdiction over Defendant because its principal place of business is in this District, regularly conducts business in California, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Defendant's principal place of business is in this District.

IV. FACTUAL ALLEGATIONS

A. The Data Breach and Defendant's Belated Notice

21. On or about June 30, 2023, Entertainment Partners identified unusual activity on its computer network, indicating a possible data breach. Following an investigation, Entertainment Partners determined that cybercriminals had infiltrated its inadequately protected network and acquired database files con containing the sensitive and personal information of Plaintiff and Class members ("Data Breach" or "Breach").[4]

22. According to Entertainment Partners, the personal information acquired by cybercriminals in the Data Breach includes names, addresses, Social Security numbers, and/or tax identification numbers ("PII" or "Personal Information") of at least 471,362 individuals.[5]

[4] https://oag.ca.gov/system/files/Sample%20Individual%20Notice.pdf.

[5] https://apps.web.maine.gov/online/aeviewer/ME/40/6dd29d7e-9e44-4ad0-9d48-1e0bd6122ab6.shtml.

23. Based on the Notice received by Plaintiff, the type of cyberattack involved, and public news reports, it is plausible and likely that Plaintiff's Personal Information was stolen in the Data Breach.

24. Upon information and belief, the unauthorized third-party cybercriminal gained access to and even "acquired" the Personal Information of Plaintiff and Class members and has engaged in (and will continue to engage in) misuse of the Personal Information, including marketing and selling Plaintiff's and Class members' Personal Information on the dark web.

25. Accordingly, Defendant had obligations created by industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiff and Class members' Personal Information confidential and to protect such Personal Information from unauthorized access.

26. Nevertheless, Defendant failed to spend sufficient resources on encryption of sensitive PII. Defendant further failed to spend sufficient resources on preventing external access, detecting outside infiltration, and preventing the exfiltration of sensitive data.

27. The stolen Personal Information at issue has great value to the hackers, due to the large number of individuals affected and the fact the sensitive information that was part of the data that was compromised.

B. Plaintiff's Experience

28. Plaintiff entrusted her Personal Information to Entertainment Partners in order to receive employment.

29. Plaintiff provided her Personal Information to Entertainment Partners with the reasonable expectation that Entertainment Partners would protect and maintain the confidentiality of the Personal Information entrusted to it.

30. Plaintiff received a notice letter from Defendant in August 2023, informing her that her Personal Information was identified as having been exposed to cybercriminals in the Data Breach.

31. Plaintiff provided her Personal Information, including her Social Security number and other information, to Defendant and trusted that Defendant would use reasonable measures to protect it. Plaintiff expected that her sensitive PII would be protected according to state and federal law and any applicable internal policies at Entertainment Partners.

32. Because of the Data Breach, Plaintiff's Personal Information is now in the hands of cybercriminals. Plaintiff and all Class members are now imminently at risk of crippling future identity theft and fraud.

33. Further, as a result of the Data Breach, Plaintiff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, researching how best to ensure that she is protected from identity theft, reviewing account statements and other information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach.

34. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Personal Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Personal Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Personal Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Personal Information; and (e) continued risk to Plaintiff's Personal Information, which remains in the possession of Defendant and which is subject to further

breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information that was entrusted to Defendant.

C. Defendant had an Obligation to Protect Personal Information under the Law and the Applicable Standard of Care

35. Defendant also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

36. Defendant is further required by various states' laws and regulations to protect Plaintiff's and Class members' Personal Information.

37. Defendant owed a duty to Plaintiff and the Class to design, maintain, and test its computer and application systems to ensure that the Personal Information in its possession was adequately secured and protected.

38. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession, including adequately training its employees (and others who accessed Personal Information within its computer systems) on how to adequately protect Personal Information.

39. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a breach on its systems in a timely manner.

40. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

41. Defendant owed a duty to Plaintiff and the Class to disclose if its computer systems and data security practices were inadequate to safeguard

individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal Information with Defendant.

42. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

43. Defendant owed a duty of care to Plaintiff and the Class because it was a foreseeable victim of a data breach.

D. Defendant was on Notice of Cyber Attack Threats and of the Inadequacy of their Data Security

44. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[6] Yahoo,[7] Marriott International,[8] Chipotle, Chili's, Arby's,[9] and others.[10]

45. Defendant should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the PII that it collected and maintained.

46. Defendant was also on notice of the importance of data encryption of Personal Information. Defendant knew it kept Personal Information in its systems

---

[6] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[7] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[8] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[9] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[10] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

and yet it appears Defendant did not encrypt these systems or the information contained within them.

E. Cyber Criminals Will Use Plaintiff's and Class Members' Personal Information to Defraud Them

47. Plaintiff and Class members' Personal Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune.

48. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[11] For example, with the Personal Information stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, collect government benefits, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[12] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

49. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[13]

50. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit

[11] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[12] https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/.

[13] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737#:~:text=Personal%20Information%3A%20Data%20Breaches%20Are,Extent%20Is%20Unknown%20%7C%20U.S.%20GAO.

card information in a retailer data breach because there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

51. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[14]

52. This was a financially motivated Data Breach, as apparent from the discovery of the cyber criminals seeking to profit off the sale of Plaintiff's and the Class members' Personal Information on the dark web. The Personal Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

53. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[15]

54. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

---

[14] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x- price-of-stolen-credit-card-numbers.html.

[15] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[16] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-

55. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[17]

56. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

57. Victims of the Data Breach, like Plaintiff and other Class members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[18]

58. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

59. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal Information;

b. Improper disclosure of their Personal Information;

737#:~:text=Personal%20Information%3A%20Data%20Breaches%20Are,Extent%20Is%20Unknown%20%7C%20U.S.%20GAO.

[17] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

[18] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal Information being placed in the hands of criminals and having been already misused;

d. The imminent and certainly impending risk of having their Personal Information used against them by spam callers to defraud them;

e. Damages flowing from Defendant's untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Personal Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

60. Moreover, Plaintiff and Class members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiff's and Class members' Personal Information.

61. Plaintiff and Class members are desperately trying to mitigate the damage that Defendant has caused them but, given the Personal Information Defendant made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Personal Information, Plaintiff and all Class members will need to have identity theft monitoring protection for the rest of their lives.

62. None of this should have happened. The Data Breach was preventable.

F. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' Personal Information

63. Data breaches are preventable.[19] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[20] she added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[21]

64. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[22]

65. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

---

[19]Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[20]*Id.* at 17.

[21]*Id.* at 28.

[22]*Id.*

According to the FTC, the need for data security should be factored into all business decision-making.

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.7 The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[23]

67. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

[23] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

69. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

70. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

71. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Personal Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

72. Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

73. Defendant was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of Plaintiff's and Class Members' Personal Information.

74. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiff's and Class members' Personal Information.

75. Defendant was at all times fully aware of its obligation to protect the Personal Information of Plaintiff and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

76. Defendant maintained the Personal Information in a reckless manner. In particular, the Personal Information was maintained and/or exchanged, unencrypted, in Defendant's systems and were maintained in a condition vulnerable to cyberattacks.

77. Defendant knew, or reasonably should have known, of the importance of safeguarding Personal Information and of the foreseeable consequences that would occur if Plaintiff's and Class members' Personal Information was stolen, including the significant costs that would be placed on Plaintiff and Class members as a result of a breach.

78. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class members' Personal Information from those risks left that information in a dangerous condition.

79. Defendant disregarded the rights of Plaintiff and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class members' Personal Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

V. CLASS ACTION ALLEGATIONS

80. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein. Plaintiff brings all claims as class claims Rule 23(b)(2), 23(b)(3) and 23(c)(4) of the Federal Rules of Civil Procedure. Plaintiff asserts all claims on behalf of the Class, defined as follows:

> All persons residing in the United States whose personal information was compromised as a result of the Entertainment Partners Data Breach, including those individuals who received breach notification letters (the "Class").
>
> All residents of California whose personal information was compromised as a result of the Entertainment Partners Data Breach, including those individuals who received breach notification letters (the "California Subclass").

The "Class" and the "California Subclass" are sometimes collectively referred to herein as the "Classes" or the "Class").

81. Plaintiff reserves the right to amend the above definitions or to propose other subclasses in subsequent pleadings and motions for class certification.

82. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class wide relief because Plaintiff and all members of the Class were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

83. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable. The proposed Subclass is also believed to be so numerous that joinder of all members would be impractical.

84. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because

Plaintiff and each member of the Class had their sensitive Personal Information compromised in the same way by the same conduct of Defendant.

85. **Adequacy:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class and proposed Subclass that she seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

86. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

87. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Personal Information;

c. Whether Defendant's email and computer systems and data security practices used to protect Plaintiff's and Class members' Personal Information violated the FTC Act, and/or state laws and/or Defendant's other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Personal Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiff and the Class to use reasonable care in protecting their Personal Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Defendant continues to breach duties to Plaintiff and the Class;

j. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

k. Whether Plaintiff and the Class are entitled to recover damages and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class and the general public;

m. Whether Defendant's actions alleged herein constitute gross negligence; and

n. Whether Plaintiff and Class members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

NEGLIGENCE

88. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

89. Defendant solicited, gathered, and stored the Personal Information of Plaintiff and the Class as part of the operation of its business.

90. Upon accepting and storing the Personal Information of Plaintiff and Class members, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

91. Defendant had full knowledge of the sensitivity of the Personal Information, the types of harm that Plaintiff and Class members could and would suffer if the Personal Information was wrongfully disclosed, and the importance of adequate security.

92. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices on the part of Defendant. Plaintiff and the Class members had no ability to protect their Personal Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

93. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive personal information.

94. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

95. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

96. Defendant had duties to protect and safeguard the Personal Information of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Personal Information. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, email accounts, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' Personal Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' Personal Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its business email system, networks and servers; and

d. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal Information.

97. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Personal Information that Plaintiff and the Class had entrusted to it.

98. Defendant breached its duty of care by failing to adequately protect Plaintiff's and Class members' Personal Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Personal Information in its possession;

b. Failing to protect the Personal Information in its possession by using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Personal Information;

d. Failing to adequately train its employees to not store Personal Information in for longer than absolutely necessary;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's Personal Information;

f. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

g. Failing to promptly and comprehensively notify Plaintiff and Class members of the Data Breach that affected their Personal Information.

99. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

100. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

101. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Personal Information of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Personal Information of Plaintiff and Class members while it was within Defendant's possession and control.

102. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps toward securing their Personal Information and mitigating damages.

103. As a result of the Data Breach, Plaintiff and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to fraudulent activity, closely monitoring bank account activity, and examining credit reports and statements sent from providers and their insurance companies.

104. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

105. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

106. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft are the types of harm that these statutes and regulations intended to prevent.

107. Defendant violated these statutes when it engaged in the actions and omissions alleged herein, and Plaintiff's and Class members' injuries were a direct and proximate result of Defendant's violations of these statutes. Plaintiff therefore is entitled to the evidentiary presumptions for negligence *per se*.

108. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the Personal Information of Plaintiff and the Class.

109. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

110. Defendant gathered and stored the Personal Information of Plaintiff and the Class as part of its business of soliciting and facilitating its services to its patients, which affect commerce.

111. Defendant violated the FTC Act by failing to use reasonable measures to protect the Personal Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

112. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data

security practices to safeguard Plaintiff's and Class members' Personal Information, and by failing to provide prompt and specific notice without reasonable delay.

113. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

114. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

115. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Personal Information.

116. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

117. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

118. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence.

119. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

SECOND CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

120. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

121. Plaintiff and the Class entrusted their Private Information to Defendant in order to receive and maintain employment. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and

confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

122. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

123. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

124. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

125. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

THIRD CAUSE OF ACTION

VIOLATIONS OF CALIFORNIA'S CONSUMER PRIVACY ACT, Cal. Civ. Code § 1798.100, et seq. ("CCPA") (On Behalf of Plaintiff and the California Subclass)

126. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

127. Defendant violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent the Personal Information of Plaintiff and the California Subclass from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

128. The non-redacted and non-encrypted Personal Information of Plaintiff and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendant' violations of their duty under the CCPA.

129. Plaintiff and the California Subclass lost money or property, including but not limited to the loss of legally protected interest in the confidentiality and privacy of their Personal Information, nominal damages, and additional losses as a direct and proximate result of Defendant' acts described above.

130. Defendant knew, or should have known, that their network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the Personal Information so in the event of a data breach an unauthorized third party cannot read the PII. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiff and members of the California Subclass was exposed.

131. Defendant is organized for the profit or financial benefit of their owners and collect PII as defined in Cal. Civ. Code § 1798.140.

132. Plaintiff the California Subclass seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguard PII by implementing reasonable security procedures and practices. This relief is important because Defendant still hold PII related to Plaintiff and the California Subclass.

Plaintiff and the California Subclass have an interest in ensuring that their PII is reasonably protected.

133. At this time, Plaintiff and California Class Members seek only actual pecuniary damages suffered as a result of Defendant's violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and any other relief the court deems proper.

134. Concurrently with the filing of this Complaint, Plaintiff is providing written notice to Defendant identifying the specific provisions of this title she alleges it has violated. If within 30 days of Plaintiff's written notice to Defendant it fails to "actually cure" its violations of Cal. Civ. Code § 1798.150(a) and provide "an express written statement that the violations have been cured and that no further violations shall occur," Plaintiff will amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

FOURTH CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80 *et seq*
(On Behalf of Plaintiff and the California Subclass)

135. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

136. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

137. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall

implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

138. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

139. Plaintiff and members of the California subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant, directly and/or indirectly, for the purpose of obtaining a service from Defendant.

140. The Personal Information of Plaintiff and the California Subclass at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collect and which was impacted by the cybersecurity attack includes an individual's name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) social security number; (ii) driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

141. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California subclass's

personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California subclass. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the California subclass from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the California subclass's nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

142. As a direct and proximate result of Defendant' violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the California subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the California subclass by the cyber attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

143. As a direct and proximate result of Defendant' acts or omissions, Plaintiff and the California subclass were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

144. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal

information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

145. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. the date of the breach,

ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected

person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

141. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all California Subclass Members. Because not all members of the class have been notified of the breach, members could have taken action to protect their personal information but were unable to do so because they were not timely notified of the breach.

142. As a direct consequence of the actions as identified above, Plaintiff and the California subclass members incurred losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, restitution, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. Ordering that Defendant cease transmitting Personal Information via unencrypted email;

vi. Ordering that Defendant cease storing Personal Information in email accounts;

vii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

viii. Ordering that Defendant conduct regular database scanning and securing checks;

ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

x. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

DATED: August 23, 2023

/s/ John J. Nelson
John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Wills Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
Email: abm@murphylegalfirm.com

**Pro Hac Vice application to be submitted*

Counsel for Plaintiff and the Proposed Class